Re Box No. V

1 Reference is made to the following document:

D1: EP1076279

2 The present application does not meet the requirements of Article 33(2) PCT, because the subject matter of claims 1 and 10 is not novel.

2.1 Document D1 discloses:

Claim 1	**Document D1**
A method for granting an access to a computer-based object, wherein	"controlling the installation and/or use of data on computer platforms" (paragraph 1)
a memory card having a program code processor is provided, with at least one public and one private key assigned to the memory card being stored thereon,	"the platform may include a ... trusted module (smart card)" (paragraph 26) "the unlock key ... is encrypted by C (=third party) using the trusted module's public key" (paragraph 69) "a trusted module ... stores a third party's public key" (paragraph 8)
an item of license information which comprises at least one license code encrypted by means of the public key assigned to the memory card is provided at a computing device controlling the access to the computer-based object,	"the unlock key is used to allow the protected data to be decrypted and run ... using a public key infrastructure to encrypt a message containing an unlock key, and checking for integrity via hashing and digital signatures..." (paragraph 12, 37, 43, 46, 56, 65-69)

a symmetric key which is made available to the memory card and the computing device is generated from a first random number generated by the memory card and from a second random number provided by the computing device,	"...setting up shared symmetric keys... The sender generates a DES key - using a random number generator, and making sure these keys are only used once" (paragraph 171)
the encrypted license code and a specification, provided with a hash value encrypted using the symmetric key, of a function that is to be executed by the memory card for decrypting the license code are transmitted to the memory card,	"Both the data and the software executor are hashed and signed with the clearinghouse/developer's private key" (paragraph 27)
the encrypted hash value is decrypted by the memory card and checked for agreement with a hash value computed for the specification of the function to be executed by the memory card,	"The secure loader integrity checks the software executor when it is received" (paragraph 27)
if the result of the check is positive, the function for decrypting the license code is executed by the memory card and a decrypted license code is transmitted to the computing device, the decrypted license code is provided at least temporarily for accessing the computer-based object.	"Optionally, applications may be run within a smart card." (paragraph 157) "When the user wishes to run the data, the secure executor decrypts the data using the unlock key and allows the data to run." (paragraph 160)

3 The independent claim 10 essentially corresponds to the method claim 1. The corresponding objections to claim 1 therefore apply also to the independent claim 10.

4 The dependent claims 2 to 9 also do not meet the requirements of Article 33 PCT, since they are neither novel nor inventive compared to D1.